WHAT IS CLAIMED IS:

1. A method of authenticating first and second electronic devices, comprising:

upon link set-up over a short-range wireless link, executing an authentication protocol by exchanging authentication information between the first and second electronic devices to initially authenticate communication between the first and second devices;

later, when the first and second electronic devices are beyond the short-range wireless link, executing the authentication protocol by exchanging the authentication information between the first and second electronic devices over an alternate communications link, then only allowing communication between the first and second devices if the first and second devices had initially been successfully authenticated.

2. The method of Claim 1, wherein the authentication information is an authentication key.

3. The method of Claim 1, wherein the authentication information a password.

4. The method of Claim 1, wherein the first device is a master device and the second device is a slave device.

5. The method of Claim 1, wherein the short-range wireless link is a radio link.

6. The method of Claim 1, wherein the short-range wireless link is an infra-red link.

7. The method of Claim 1, wherein the link set-up occurs when the first and second devices are in physical proximity.

8. The method of Claim 1, wherein the short-range wireless link conforms to a given RF protocol.

9. The method of Claim 2, wherein the given RF protocol is Bluetooth.

10. The method of Claim 1 wherein the link set-up step includes entry of a given personal identification number into each of the first and second electronic devices.

11. The method of Claim 1, wherein the alternate communications link is a computer network.

12. The method of Claim 1, wherein the first electronic device is a client and the second electronic device is a server.

13. A method of authenticating first and second electronic devices, comprising:

upon link set-up over a first link, executing an authentication protocol by exchanging authentication information between the first and second electronic devices to initially authenticate communication between the first and second devices;

later, when the first and second electronic devices are connected using a second link, exchanging the authentication information between the first and second electronic devices over the second link, then only allowing communication between the first and second

devices if the first and second devices had initially been successfully authenticated.

14. An electronic device, comprising:

a processor;

and

a memory loaded with a software routine executed by the processor (a) for generating authentication information useful in initially authenticating the electronic device to a another electronic device over a short-range wireless link, and (b) for later supplying the authentication information for later authentication of the electronic device to the otherelectronic device over an alternate communications link when the devices are beyond the short-range wireless link, then only allowing communication between the devices if the devices had initially been successfully authenticated.

15. The electronic device of Claim 14, wherein the link set-up step includes entry of a given personal identification number into each of the first and second electronic devices.

16. The electronic device of Claim 14, wherein the electronic device is a client and the second electronic device is a server.

17. A communications system, comprising:

a first electronic device;

a second electronic device;

a first communications link over which the first and second electronic devices authenticate each other using a given protocol that includes a link set-up and the exchange of authentication information following the link

set-up, the authentication information being used to initially authenticate communication between the first and second electronic devices; and

a second communications link over which the first and second electronic devices later authenticate each other using the exchange of the authentication information, then only allowing communication between the first and second devices if the first and second devices had initially been successfully authenticated.